Here is some information about the security of Dropbox and other services.

From the Dropbox website:

Is Dropbox safe to use?

At Dropbox, the security of your data is our highest priority. We have a dedicated security team using the best tools and engineering practices available to build and maintain Dropbox, and you can rest assured that we've implemented multiple levels of security to protect and back up your files. You can also take advantage of two-step verification, a login authentication feature which you can enable to add another layer of security to your account.

Other Dropbox users can't see your files in Dropbox unless you share links to files or share folders. Like most online services, we have a small number of employees who must be able to access user data for the reasons stated in our privacy policy (e.g., when legally required to do so). But that's the rare exception, not the rule. We have strict policy and technical access controls that prohibit employee access except in these rare circumstances. In addition, we employ a number of physical and logical security measures to protect user information from unauthorized access.

For our advanced users

- Dropbox files at rest are encrypted using 256-bit Advanced Encryption Standard (AES).
- Dropbox uses Secure Sockets Layer (SSL)/Transport Layer Security (TLS) to protect data in transit between Dropbox apps and our servers; it's designed to create a secure tunnel protected by 128-bit or higher Advanced Encryption Standard (AES) encryption.
- Dropbox applications and infrastructure are regularly tested for security vulnerabilities and hardened to enhance security and protect against attacks.
- Two-step verification is available for an extra layer of security at login. You can choose to receive security codes by text message or via any Time-Based One-Time Password (TOTP) apps, such as those listed here.
- Public files are only viewable by people who have a link to the file(s).

Dropbox is designed with multiple layers of protection, including secure data transfer, encryption, network configuration, and application- and user-level controls that are distributed across a scalable, secure infrastructure.

Security on the Hi-Rise computers

Dropbox should be secure on our computers. If a site has a computer in their office the Dropbox software will be installed there. Those hi-rises that use one of the computers in the community room for council work will have Dropbox installed in the Council or Admin account. When it is installed in one account there is no icon visible in the other accounts on the computer and those accounts can't access the Dropbox folder on the computer

Anyone accessing the admin account on a council computer will have access to the Dropbox folder and the files it contains. This shouldn't be an issue because there shouldn't be anything in that folder that the other officers shouldn't see. If there is a concern about that it might be better to uninstall the Dropbox software from the computer and just upload files via the Dropbox website. Passwords can also be changed more regularly.

Dropbox vs other cloud storage sites

From what I have seen, the security is comparable at sites such as Onedrive, Google Drive, iCloud Drive, and Box. (Box does have some more security options for business users.)

The advantage to Dropbox is the ease in transferring files from multiple accounts to the Presidents Council account downtown.

With Dropbox each hi-rise has their own account and the Presidents Council has an account. The Presidents Council has access to one folder from each account. The hi-rises only have access to their own folders and files.

With other sites such as Box or Onedrive we would have to have one account that every hi-rise and the Presidents Council would use. Everyone would log into that account and upload files to their folders. (You can still have multiple folders in other cloud storage services.)

The issue with that (along with having one shared account for everybody and all the security concerns that would bring with it) is that every folder and file uploaded to that account (say Onedrive) would be duplicated on any computer logged into that account. That means that if I'm logged into the shared Onedrive account here at Seal I would have copies of every hi-rise's work on our office computer. Every other hi-rise would also have copies of all 16 hi-rises' work. I'm sure we don't want that.

Dropbox allows us to avoid that and is easy for people to use.

I have investigated a number of other services and I have not found another that offers Dropbox's functionality. (With shared folders specifically.)

How to make things more secure

Here are some options for increasing security.

1. Two factor authentication. This means that when the Dropbox account is logged into as well as entering the password you would need to enter a code that would be texted to your phone. This is good at preventing unauthorized access. It also can be a pain in the neck and cause a whole host of problems. If you have two factor authentication turned on and lose your phone or change the number you will not be able to get the code and will not be able to access your account. There may be alternate ways to regain access but that usually requires jumping through a bunch of hoops and it is a pain and takes time. I don't recommend this option since there may be multiple people who need to access the Dropbox accounts and because of the potential for issues.
2. Encrypting files. There are a number of software programs that can do this before files are uploaded to a storage service or sent in an email. This would prevent unauthorized access both from people on our and and people from the cloud service. It also would

require extra work and there is the potential for issues if files have to be decrypted. (Also the learning curve for users who have never used that type of software before.) I don't believe encryption is necessary in our situation because the files we are uploading are not that sensitive and we aren't subject to regulations like HIPPA.

3. Regular password changes. This would be a good idea. Especially if there is concern about residents accessing the accounts.
4. Not having the software on the computers and just using the website. This isn't quite as convenient but it might be more secure if there are concerns about computers in the community rooms or access from other board members.